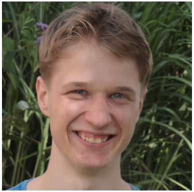
Skolem meets Schanuel

Yuri Bilu
joint work with
Florian Luca, Joris Nieuwveld, Joël Ouaknine,
David Purser, James (Ben) Worrell

Online Number Theory Seminar
January 19, 2024

My co-authors

Florian



Joris

Joël

David

Ben

Linear Recurrences

K field of characteristic 0

A map

$$U : \mathbb{Z} \to K$$

is called K-valued Linear Recurrence (LR) of order r
if $\exists a_0, \ldots, a_{r-1} \in K$, $a_0 \neq 0$ such that $\forall n \in \mathbb{Z}$

$$U(n+r) = a_{r-1}U(n+r-1) + \cdots + a_0 U(n)$$

Example: Fibonacci LR $\quad U(n+2) = U(n+1) + U(n)$

n	$\cdots$	-4	-3	-2	-1	0	1	2	3	4	5	6	$\cdots$
$U(n)$	$\cdots$	-3	2	-1	1	0	1	1	2	3	5	8	$\cdots$

Binet Formula

$\chi(T) = \chi_U(T) := T^r - a_{r-1}T^{r-1} - \cdots - a_0$ is the characteristic polynomial of the LR U. It factors as

$$\chi(T) = (T - \lambda_1)^{\nu_1} \cdots (T - \lambda_s)^{\nu_s},$$

where $\lambda_1, \dots, \lambda_s \in \bar{K}$ are distinct and called the roots of U.
Then we have the "Binet Formula"

$$U(n) = f_1(n)\lambda_1^n + \cdots + f_s(n)\lambda_s^n,$$

where $f_i(T) \in \bar{K}[T]$ satisfy $\deg f_i \leq \nu_i - 1$.
U is called simple LR if $\chi(T)$ has only simple roots: $s = r$ and $\nu_1 = \cdots = \nu_r = 1$. In this case

$$U(n) = \alpha_1\lambda_1^n + \cdots + \alpha_r\lambda_r^n, \qquad \alpha_i \in \bar{K}.$$

Example: if U is Fibonacci, then $U(n) = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}$.

Zeros of LRs

A zero of a LR U is a solution $n \in \mathbb{Z}$ of the equation $U(n) = 0$.
Question: Does every LR (which is not identically 0) have at most finitely many zeros?
No! Consider the LR of order 2 with the general term $\frac{1}{2}\left(1^n + (-1)^n\right)$:

$$\ldots, 1, 0, 1, 0, 1, \ldots$$

Call U non-degenerate if λ_i/λ_j is not a root of unity for $i \neq j$.
For every LR U there exists N such that each of the N LRs

$$V_k(n) := U(k + Nn) \qquad (k = 0, 1, \ldots, N-1)$$

is either non-degenerate or identically 0. So it suffices to study the zeros of non-degenerate LRs.

The Skolem-Mahler-Lech Theorem

Theorem (Skolem 1933, Mahler 1935, Lech 1953) Let U be a non-degenerate LR with values in a field K of characteristic 0. Then U has at most finitely many zeros.

Two methods of proof:

- using p-adic interpolation (Skolem etc., inspired important later work of Chabauty-Coleman-Kim etc.);
- using the Subspace Theorem (was extended by M. Laurent etc.).

Skolem's argument will be sketched later in this talk.

Both methods are non-effective. In particular, the p-adic method is non-effective, because knowing a p-adic integer approximately with any given precision does not allow one to decide whether it is a rational integer ($\mathbb{Z}$ is dense in $\mathbb{Z}_p$).

Skolem Problems

Let K be a **number field**.
Weak Skolem Problem (WSP): decide whether a given K-valued non-degenerate LR U admits a zero.

Strong Skolem Problem (SSP): determine all the zeros of a given K-valued non-degenerate LR U.

Both problems are currently not known to have an effective solution. By an effective solution we understand an **algorithm** solving the problem, together with an explicit **estimate for the running time** in terms of the initial data (in our case the terms $U(0), \dots, U(r-1)$ and the coefficients $a_0, \dots, a_{r-1}$).

However, the **SSP can be solved effectively in many special cases, using "dominant roots".**

From now on, U is a **simple non-degenerate LR** with values in a number field K:

$$U(n) = \alpha_1 \lambda_1^n + \cdots + \alpha_r \lambda_r^n.$$

Extending K, we may assume that $\lambda_1, \dots, \lambda_r, \alpha_1, \dots, \alpha_r \in K^\times$.

Dominant Roots

Let $v \in M_K$. We say that U admits a v-dominant root if the roots $\lambda_1, \ldots, \lambda_r$ can be numbered to have

$$|\lambda_1|_v > |\lambda_2|_v \geq \cdots \geq |\lambda_r|_v.$$

Proposition. If U admits a v-dominant root for some $v \in M_K$ then the zeros $n \geq 0$ can be effectively determined.

Proof. For sufficiently large $n > 0$

$$|\alpha_1 \lambda_1^n|_v > |\alpha_2 \lambda_2^n + \cdots + \alpha_r \lambda_r^n|_v. \qquad \square$$

Similarly, if U admits a v-antidominant root, that is, for some numbering we have $|\lambda_1|_v < |\lambda_2|_v \leq \cdots \leq |\lambda_r|_v$ then the zeros $n \leq 0$ can be effectively determined.

Corollary If U admits a v-dominant root for some $v \in M_K$, and a v'-antidominant root for some $v' \in M_K$ then the SSP for U can be solved effectively.

Dominant Roots II

We say that U admits two v-dominant roots if the roots can be numbered to have

$$|\lambda_1|_v = |\lambda_2|_v > |\lambda_3| \geq \cdots \geq |\lambda_r|_v .$$

The previous argument no longer works. But $|\alpha_1\lambda_1^n + \alpha_2\lambda_2^n|_v$ cannot be too small by Baker:

$$|\alpha_1\lambda_1^n + \alpha_2\lambda_2^n|_v = |\alpha_1\lambda_1^n|_v \left| \frac{\alpha_2}{\alpha_1}\left(\frac{\lambda_2}{\lambda_1}\right)^n - 1 \right|_v \geq |\alpha_1\lambda_1^n|_v e^{-O(\log n)}.$$

Hence, for sufficiently large $n > 0$

$$|\alpha_1\lambda_1^n + \alpha_2\lambda_2^n|_v > |\alpha_3\lambda_3^n + \cdots + \alpha_r\lambda_r^n|_v .$$

Thus, if U admits two v-dominant roots for some $v \in M_K$ then the zeros $n \geq 0$ can be effectively determined.

Dominant Roots III

Corollary. SSP can be effectively solved for all simple non-degenerate LR of order ≤ 3.

Proof. It is not possible to have $|\lambda_1|_v = |\lambda_2|_v$ for all $v \in M_K$ because λ_1/λ_2 is not a root of unity. Hence for some v the 3 numbers $|\lambda_1|_v, |\lambda_2|_v, |\lambda_3|_v$ are not all equal, and we have one of the following three options:
- a v-dominant root and a v-antidominant root;
- two v-dominant roots and a v-antidominant root;
- a v-dominant root and two v-antidominant roots. □

In a similar, but more tricky fashion (using a trick due to Beukers) one proves

Theorem. (Mignotte-Shorey-Tijdeman 1984, Vereshchagin 1985). SSP can be effectively solved for all simple non-degenerate LR of order ≤ 4, taking real algebraic values.

However, at present, the dominant roots method does not allow to solve SSP for general LRs of order ≥ 5, and for LRs of order 4 with non-real values.

Conditional Algorithms

Our principal results are.

- An algorithm, which, when terminates, solves the WSP. Moreover, it produces a zero if there is one. This algorithm always terminates subject to the **Exponential Local-Global Principle**.
- An algorithm, which, when terminates, solves the SSP: it produces the full list of zeros of a given (simple non-degenerate) LR, and a rigorous proof of non-existence of further zeros. This algorithm always terminates subject to the **Exponential Local-Global Principle** and the ***p*-adic Schanuel Conjecture**.

Unfortunately, we do not obtain, even conditionally, any estimate for the running time. But the algorithms perform well in practice.

Exponential Local-Global Principle

Let S be a finite subset of M_K, and $\mathcal{O}_S$ the ring of S-integers in K.

Let $\mathcal{U}$ a set of simple LRs U with general term

$$U(n) = \alpha_1 \lambda_1^n + \cdots + \alpha_r \lambda_r^n$$

where $\alpha_1, \ldots, \alpha_r \in \mathcal{O}_S$ and $\lambda_1, \ldots, \lambda_r \in \mathcal{O}_S^\times$.

We say that the set $\mathcal{U}$ satisfies the Exponential Local-Global Principle (ELGP) if $\forall U \in \mathcal{U}$ one of the following holds:

- either $\exists n \in \mathbb{Z}$ such that $U(n) = 0$,
- or there is a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_S$ such that

$$\forall n \in \mathbb{Z} \qquad U(n) \not\equiv 0 \mod \mathfrak{a}.$$

Remark: ELGP does not extend to non-simple LRs, because the Local-Global Principle does not hold for polynomials. For example, the polynomials $(T^2 - 13)(T^2 - 17)(T^2 - 221)$ and $(T^3 - 19)(T^2 + T + 1)$ have a root modulo every integer, but not a root in $\mathbb{Q}$.

Algorithm for Weak Skolem Problem

Run simultaneously

- search for $n \in \mathbb{Z}$ such that $U(n) = 0$, and
- search for a non-zero ideal $\mathfrak{a}$ such that U does not vanish $\bmod \mathfrak{a}$.

If the algorithm terminates, it produces either a zero of U, or a rigorous proof of non-existence of a zero.

Assuming the ELGP, the algorithm always terminates.

p-adic $\log$ and $\exp$

$p \geq 3$ a prime number. For $z \in \mathbb{Z}_p$ satisfying $|z|_p < 1$ define

$$\exp(z) := \sum_{n=0}^{\infty} \frac{z^n}{n!}.$$

For $z \in \mathbb{Z}_p$ satisfying $|z-1|_p < 1$ define

$$\log(z) := \sum_{n=1}^{\infty} (-1)^{n-1} \frac{(z-1)^n}{n}.$$

Then

$$|\exp(z) - 1|_p = |z|_p, \qquad |\log(z)|_p = |z-1|_p,$$

and all familiar properties are satisfied.

p-adic Interpolation of a LR

- K a number field;
- $U(n) = \alpha_1\lambda_1^n + \cdots + \alpha_r\lambda_r^n, \quad \alpha_i, \lambda_i \in K^\times$.

Let $p \geq 3$ be a prime number such that

$$K \hookrightarrow \mathbb{Q}_p, \qquad \lambda_i \in \mathbb{Z}_p^\times, \qquad \alpha_i \in \mathbb{Z}_p.$$

There are infinitely many such p.

Want to define $U(z)$ for all $z \in \mathbb{Z}_p$.

Need to define λ_i^z. The straightforward $\lambda_i^z := \exp(z \log \lambda_i)$ does not work, because we need $|\lambda_i - 1|_p < 1$ to define $\log \lambda_i$.

Little Fermat: $|\lambda_i^{p-1} - 1|_p < 1$.

For $k \in \{0, 1, \ldots, p-2\}$ we may define

$$\lambda_i^{k+z(p-1)} := \lambda_i^k \exp\bigl(z \log(\lambda_i^{p-1})\bigr)$$

p-adic Interpolation of a LR II

Theorem. For $k = 0, 1, \ldots, p-2$ define

$$g_k(z) := \sum_{i=1}^{r} \alpha_i \lambda_i^k \exp\bigl(z \log(\lambda_i^{p-1})\bigr).$$

Then $g_k : \mathbb{Z}_p \to \mathbb{Z}_p$ is an analytic function, satisfying

$$g_k(m) = U(k + m(p-1)) \qquad (m \in \mathbb{Z}).$$

If U is non-degenerate, then the functions g_k are not identically 0.

Corollary. (Skolem-Mahler-Lech) If U is non-degenerate then equation $U(n) = 0$ has at most finitely many solutions in $n \in \mathbb{Z}$.

Proof. Equation $g_k(z) = 0$ has at most finitely many solutions in $z \in \mathbb{Z}_p$, because $\mathbb{Z}_p$ is compact and the set of solutions is discrete (the zeros of an analytic function are "isolated").

Remark. The Skolem-Mahler-Lech Theorem extends to arbitrary K of characteristic 0 using the Lech-Cassels Embedding Theorem.

The p-adic Schanuel conjecture

Classical Schanuel Conjecture. if $\beta_1, \dots, \beta_s \in \mathbb{C}$ are linearly independent over $\mathbb{Q}$, then the field $\mathbb{Q}(\beta_1, \dots, \beta_s, e^{\beta_1}, \dots, e^{\beta_s})$ is of transcendence degree $\geq s$ (over $\mathbb{Q}$).

Known in the case when $\beta_1, \dots, \beta_s \in \bar{\mathbb{Q}}$ (Lindemann-Weierstrass), and in some special cases, but widely open in general.

***p*-adic Schanuel Conjecture.** if $\beta_1, \dots, \beta_s \in p\mathbb{Z}_p$ are linearly independent over $\mathbb{Q}$, then the field $\mathbb{Q}(\beta_1, \dots, \beta_s, \exp(\beta_1), \dots, \exp(\beta_s))$ is of transcendence degree $\geq s$.

A special case: If $\gamma_1, \dots, \gamma_s \in 1 + p\mathbb{Z}_p$ are **algebraic over** $\mathbb{Q}$ and **multiplicatively independent**, then the $\log \gamma_1, \dots, \log \gamma_s$ are algebraically independent over $\mathbb{Q}$.

Remark: the p-adic Schanuel is considered even harder, than the complex Schanuel; for instance, the p-adic LW is still an open problem.

Isolating a Zero in a Residue Class

Proposition. Let $a \in \mathbb{Z}$ be a zero of U. Then there exist $N \in \mathbb{Z}_{>0}$ such that $U(n) \neq 0$ for $n \equiv a \bmod N$ and $n \neq a$.

Proof. Let $k \in \{0, 1, \ldots, p-2\}$ be such that $a \equiv k \bmod p-1$. Write $a = k + b(p-1)$. Then

$$g_k(b) = U(k + b(p-1)) = U(a) = 0.$$

Since the zeros of an analytic function are isolated, there exists $\ell > 0$ such that

$$g_k(b + p^\ell z) \neq 0$$

for $z \in \mathbb{Z}_p$, $z \neq 0$. Now define $N = (p-1)p^\ell$. □

Finding N and Schanuel

To find N, we need to find ℓ such that the analytic function $z \mapsto g_k(b+z)$ does not vanish in in the pierced disk $0 < |z|_p \leq p^{-\ell}$. The problem reduces to finding the first non-zero coefficient in the Taylor expansion

$$g_k(b+z) = c_1 z + c_2 z_2 + \cdots .$$

The coefficients are polynomials in $\log \gamma_i$, where $\gamma_i := \lambda_i^{p-1}$. We may assume that $\lambda_1, \ldots, \lambda_s$, $s \leq r$, is a maximal multiplicatively independent subset of $\lambda_1, \ldots, \lambda_r$. Then the coefficients are polynomials in $\log \gamma_1, \ldots, \log \gamma_s$:

$$c_j = P_j\big(\log \gamma_1, \ldots, \log \gamma_s\big), \qquad P_j \in K[T_1, \ldots, T_s].$$

The p-adic Schanuel implies the following: $c_i = 0$ iff P_i is an identically zero polynomial.

Thus, assuming Schanuel, finding N reduces to the finding the smallest i such that P_i is not identically zero.

Algorithm for Solving the Strong Skolem Problem

1. Solve the WSP for U, using the previous algorithm.
2. If U does not vanish, done.
3. If we find a zero a of U, we look for N such that a is the only zero in its residue class $\bmod N$.
4. We repeat recursively the previous steps for the $N-1$ LRs $V_k(n) := U(k+Nn)$, where k runs all the residue classes $\bmod N$ except $a \bmod N$.

Step 1 terminates assuming the ELGP, and Step 3 terminates assuming the p-adic Schanuel. Recursion also terminates because U has at most finitely many zeros, and on each stage we filter out one zero.

The algorithm is implemented in the Skolem Tool:

https://skolem.mpi-sws.org/

Example: Tribonacci sequence

$$T(0) = 0, \quad T(1) = 1, \quad T(2) = 1,$$
$$T(n+3) = T(n+2) + T(n+1) + T(n)$$

n	$\cdots$	-6	-5	-4	-3	-2	-1	0	1	2	3	$\cdots$
$T(n)$	$\cdots$	-3	2	0	-1	1	0	0	1	1	2	$\cdots$

We see that $T(0) = T(-1) = T(-4) = 0$. Also, $T(-17) = 0$

Mignotte, Tzanakis (1991): $T(n) = 0 \iff n \in \{0, -1, -4, -17\}$

Proof uses congruences (similar to our method).

Köszönöm!